

AMENDMENTS TO CLAIMS

1. (Previously presented) A method of restricting Address Resolution Protocol (ARP) table updates to updates originating from authorized subsystems, the method comprising:

receiving an instruction to update an ARP table from a particular subsystem of a network device;

determining whether the particular subsystem within the network device from which the instruction originated is authorized;

wherein determining that the particular subsystem is authorized comprises

determining that the particular subsystem is a Dynamic Host

Configuration Protocol (DHCP) server, an Authentication, Authorization,

Accounting (AAA) server or a Network Address Translator (NAT); and

only if the particular subsystem is authorized, then updating the ARP table based on the instruction.

2. (Canceled)

3. (Previously presented) The method of Claim 1, wherein determining whether the particular system is authorized comprises determining whether the particular subsystem is a Dynamic Host Configuration Protocol (DCHP) server.

4. (Previously presented) The method of Claim 1, wherein determining whether the particular system is authorized comprises determining whether the particular subsystem is a Network Address Translator (NAT).

5. (Previously presented) The method of Claim 1, wherein determining whether the particular system is authorized comprises determining whether the particular subsystem is an Authentication, Authorization, Accounting (AAA) server.

6. (Original) The method of Claim 1, further comprising:
if the particular subsystem is not authorized, then preventing the ARP table from being updated based on the instruction.

7. (Original) The method of Claim 1, further comprising:
if the particular subsystem is not authorized, then performing the steps of:
determining whether a particular network interface through which the instruction was received is contained in a set of one or more specified network interfaces;
if the particular network interface is contained in the set, then preventing the ARP table from being updated based on the instruction; and
if the particular network interface is not contained in the set, then updating the ARP table based on the instruction.

8. (Original) The method of Claim 1, further comprising:
if the particular subsystem is not authorized, then performing the steps of:
determining whether a particular network address indicated by the instruction is contained in a set of one or more specified network addresses;
if the particular network address is contained in the set, then preventing the ARP table from being updated based on the instruction; and
if the particular network address is not contained in the set, then updating the ARP table based on the instruction.

9. (Original) The method of Claim 1, further comprising:
determining whether a specified amount of time has passed since a time indicated by a
timestamp associated with an entry in the ARP table; and
if the specified amount of time has passed, then removing the entry from the ARP table.
10. (Original) The method of Claim 1, wherein the ARP table is updated only in
response to instructions that are not ARP messages.
11. (Original) The method of Claim 1, wherein determining whether the particular
system is authorized comprises determining whether the particular subsystem is a
Hypertext Transfer Protocol (HTTP) server.
12. (Currently Amended) A method of restricting Address Resolution Protocol (ARP) table
updates to updates originating from authorized subsystems, the method comprising:
receiving an instruction to update an ARP table from a network device over a particular
network interface;
determining whether the particular network interface through which the instruction was
received is contained in a set of one or more specified network interfaces;
determining whether a particular network address indicated by the instruction is
contained in a set of one or more specified network addresses;
if the particular network interface is not contained in the set of one or more specified
network interfaces, and if the particular network address indicated by the
instruction is not contained in the set of one or more specified network addresses,
then updating the ARP table based on the instruction; and

if the particular network interface is contained in the set of one or more specified network interfaces, or if the particular network address is contained in the set of one or more specified network addresses, then performing steps comprising:
determining whether a particular subsystem in a network element from which the instruction originated is authorized;
wherein determining that the particular subsystem is authorized comprises
determining that the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT);
only if the particular subsystem is authorized, then updating the ARP table based on the instruction; and
if the particular subsystem is not authorized, then preventing the ARP table from being updated based on the instruction.

13. (Original) The method of Claim 12, wherein receiving the instruction to update the ARP table comprises receiving an ARP message that indicates an association between a network layer address and a data link layer address.

14.-22. (Canceled)

23. (Currently Amended) A computer-readable storage medium ~~carrying~~ storing one or more sequences of instructions for restricting Address Resolution Protocol (ARP) table updates to updates originating from authorized subsystems, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving an instruction to update an ARP table from a particular subsystem of a network device;

determining whether the particular subsystem within the network device from which the instruction originated is authorized;

wherein the step of determining that the particular subsystem is authorized

comprises determining that the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT); and

only if the particular subsystem is authorized, then updating the ARP table based on the instruction.

24. (Currently Amended) An apparatus for restricting Address Resolution Protocol (ARP) table updates to updates originating from authorized subsystems, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

one or more processors;

means for receiving an instruction to update an ARP table from a particular subsystem of a network device;

means for determining whether the particular subsystem within the network device from which the instruction originated is authorized;

wherein the means for determining that the particular subsystem is authorized

comprises means for performing said determining by determining that the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT); and

means for updating the ARP table based on the instruction only if the particular subsystem is authorized.

25. (Previously presented) An apparatus for restricting Address Resolution Protocol (ARP) table updates to updates originating from authorized subsystems, comprising:
a network interface that is coupled to a data network for receiving one or more packet flows therefrom;
a processor; and
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving an instruction to update an ARP table from a particular subsystem of a network device;
determining whether the particular subsystem within the network device from which the instruction originated is authorized;
wherein determining that the particular subsystem is authorized comprises
determining that the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server, an Authentication, Authorization, Accounting (AAA) server or a Network Address Translator (NAT); and
only if the particular subsystem is authorized, then updating the ARP table based on the instruction.

26. (Canceled)

27. (Previously presented) The apparatus of Claim 24, wherein determining whether the particular system is authorized comprises determining whether the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server.

28. (Previously presented) The apparatus of Claim 24, wherein determining whether the particular system is authorized comprises determining whether the particular subsystem is a Network Address Translator (NAT).

29. (Previously presented) The apparatus of Claim 24, wherein determining whether the particular system is authorized comprises determining whether the particular subsystem is an Authentication, Authorization, Accounting (AAA) server.

30. (Previously presented) The apparatus of Claim 24, further comprising:
if the particular subsystem is not authorized, then preventing the ARP table from being updated based on the instruction.

31. (Previously presented) The apparatus of Claim 24, further comprising:
means for determining whether the particular subsystem is not authorized;
means for determining whether a particular network interface through which the
instruction was received is contained in a set of one or more specified network
interfaces;
means for preventing the ARP table from being updated based on the instruction when
the particular network interface is contained in the set; and
means for updating the ARP table based on the instruction when the particular network
interface is not contained in the set.

32. (Previously presented) The apparatus of Claim 24, further comprising:
means for determining whether the particular subsystem is not authorized;
means for determining whether a particular network address indicated by the instruction
is contained in a set of one or more specified network addresses;
means for preventing the ARP table from being updated based on the instruction when
the particular network address is contained in the set; and
means for updating the ARP table based on the instruction when the particular network
address is not contained in the set.
33. (Canceled)
34. (Previously presented) The apparatus of Claim 25, wherein the instructions which_a
when executed, cause the processor to carry out the step of determining whether the particular
system is authorized comprise instructions which_a when executed, cause the processor to carry
out the step of determining whether the particular subsystem is a Dynamic Host Configuration
Protocol (DCHP) server.
35. (Previously presented) The apparatus of Claim 25, wherein the instructions which_a
when executed, cause the processor to carry out the step of determining whether the particular
system is authorized comprise instructions which_a when executed, cause the processor to carry
out the step of determining whether the particular subsystem is a Network Address Translator
(NAT).
36. (Previously presented) The apparatus of Claim 25, wherein the instructions which_a
when executed, cause the processor to carry out the step of determining whether the particular
system is authorized comprise instructions which_a when executed, cause the processor to carry

out the step of determining whether the particular subsystem is an Authentication, Authorization, Accounting (AAA) server.

37. (Previously presented) The apparatus of Claim 25, further comprising instructions which, when executed, cause the processor to carry out the step of preventing the ARP table from being updated based on the instruction if the particular subsystem is not authorized.

38. (Previously presented) The apparatus of Claim 25, further comprising instructions which, when executed, cause the processor to carry out the steps of:
determining whether the particular subsystem is not authorized;
determining whether a particular network interface through which the instruction was received is contained in a set of one or more specified network interfaces;
preventing the ARP table from being updated based on the instruction when the particular network interface is contained in the set; and
updating the ARP table based on the instruction when the particular network interface is not contained in the set.

39. (Previously presented) The apparatus of Claim 25, further comprising instructions which, when executed, cause the processor to carry out the steps of:
determining whether the particular subsystem is not authorized;
determining whether a particular network address indicated by the instruction is contained in a set of one or more specified network addresses;
preventing the ARP table from being updated based on the instruction when the particular network address is contained in the set; and
updating the ARP table based on the instruction when the particular network address is not contained in the set.

40. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the instructions which when executed cause determining whether the particular system is authorized comprise instructions which when executed cause determining whether the particular subsystem is a Dynamic Host Configuration Protocol (DHCP) server.

41. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the instructions which when executed cause determining whether the particular system is authorized comprise instructions which when executed cause determining whether the particular subsystem is a Network Address Translator (NAT).

42. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the instructions which when executed cause determining whether the particular system is authorized comprise instructions which when executed cause determining whether the particular subsystem is an Authentication, Authorization, Accounting (AAA) server.

43. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

if the particular subsystem is not authorized, then preventing the ARP table from being updated based on the instruction.

44. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

upon determining that the particular subsystem is not authorized;
determining whether a particular network interface through which the instruction was received is contained in a set of one or more specified network interfaces;
preventing the ARP table from being updated based on the instruction if the particular network interface is contained in the set; and
updating the ARP table based on the instruction if the particular network interface is not contained in the set.

45. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

upon determining that the particular subsystem is not authorized;
determining whether a particular network address indicated by the instruction is contained in a set of one or more specified network addresses;
preventing the ARP table from being updated based on the instruction if the particular network address is contained in the set; and
updating the ARP table based on the instruction if the particular network address is not contained in the set.

46. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the one or more stored sequences of instructions, when executed by the processor, further cause the processor to perform:

determining whether a specified amount of time has passed since a time indicated by a timestamp associated with an entry in the ARP table; and
if the specified amount of time has passed, then removing the entry from the ARP table.

47. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the ARP table is updated only in response to instructions that are not ARP messages.
48. (Previously Presented) The computer-readable storage medium of Claim 23, wherein the instructions which when executed cause determining whether the particular system is authorized comprise instructions which when executed cause determining whether the particular subsystem is a Hypertext Transfer Protocol (HTTP) server.